Grassmannian Codes as Lifts of Matrix Codes Derived as Images of Linear Block Codes over Finite Fields

Bryan S. Hernandez and Virgilio P. Sison
Institute of Mathematical Sciences and Physics
University of the Philippines, Los Baños
College, Laguna 4031, Philippines
Email: {bshernandez, vpsison}@up.edu.ph

***Abstract*—Let p be a prime such that $p \equiv 2$ or 3 (mod 5). Linear block codes over the non-commutative matrix ring $M_2(\mathbb{F}_p)$ endowed with the Bachoc weight are derived as isometric images of linear block codes over the Galois field $\mathbb{F}_{p^2}$ endowed with the Hamming metric. When seen as rank metric codes, this family of matrix codes satisfies the Singleton bound and thus are maximum rank distance codes, which are then lifted to form a special class of subspace codes, the Grassmannian codes, that meet the anticode bound. These so-called anticode-optimal Grassmannian codes are associated in some way with complete graphs. New examples of these maximum rank distance codes and anticode-optimal Grassmannian codes are given.**

***Index Terms*—network coding, subspace codes, grassmannian codes, maximum rank distance codes.**

I. Introduction

This paper deals with certain concepts of "coding theory in projective space" and highlights the practical significance of subspace codes, specifically of Grassmannian codes, in error correction in networks. Let $q = p^r$, p a prime, r a positive integer, and $\mathbb{F}_q$ the Galois field with cardinality q and characteristic p. Consider the n-dimensional full vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$. The set of all subspaces of $\mathbb{F}_q^n$, denoted by $\mathcal{P}_q(n)$, is called the projective space of order n over $\mathbb{F}_q$. For an integer k, where $0 \leq k \leq n$, the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, denoted by $\mathcal{G}_q(n, k)$, is called the Grassmannian. A subspace code is a nonempty subset of $\mathcal{P}_q(n)$. A Grassmannian code is a nonempty subset of $\mathcal{G}_q(n, k)$ which is also called a constant dimension code, that is, the codewords in $\mathcal{G}_q(n, k)$ are subspaces of $\mathbb{F}_q^n$ of dimension k, thus they are nothing but rate-k/n linear block codes of length n over $\mathbb{F}_q$. Subspace codes have practical importance in network coding. The seminal paper [1] refers to *network coding* as "coding at a node in a network", that is, a node receives information from all input links, then encodes and sends information to all output links.

Section II gives important theoretical preliminaries, while Section III shows how to construct Grassmannian codes endowed with the subspace distance as lifts of certain linear block codes $\mathcal{M}$ over the non-commutative matrix ring $M_2(\mathbb{F}_p)$ endowed with the Bachoc weight. The matrix codes $\mathcal{M}$ are isometric images of linear block codes over $\mathbb{F}_{p^2}$ endowed with the Hamming distance. More importantly, these matrix codes are maximum rank distance codes, or MRD codes, that is, they satisfy the Singleton bound for matrix codes with respect to the rank metric. The Grassmannian codes constructed from these lifts are anticode-optimal, or simply optimal, in the sense that they satisfy the anticode bound. New examples of MRD codes and anticode-optimal Grassmannian codes are given from these constructions. In Section IV it is shown that this family of anticode-optimal Grassmannian codes can be associated in a peculiar way with complete graphs.

II. Preliminaries

The set of all $k \times \ell$ matrices over $\mathbb{F}_q$, denoted by $M_{k\times\ell}(\mathbb{F}_q)$, is considered as a vector space over $\mathbb{F}_q$. A nonempty subset of $M_{k\times\ell}(\mathbb{F}_q)$ is called a $[k \times \ell]$ *matrix code* over $\mathbb{F}_q$. This $[k \times \ell]$ matrix code is said to be linear if it is a subspace of $M_{k\times\ell}(\mathbb{F}_q)$.

The *rank distance* between two $k \times \ell$ matrices over $\mathbb{F}_q$, say A and B, is defined by $d_R(A, B) = \text{rank}(A - B)$, and is clearly a metric. A $[k \times \ell, \delta]$ *rank-metric code* $\mathbb{C}$ is a $[k \times \ell]$ matrix code whose minimum rank distance is δ. That is, $\delta = \min\{d_R(A, B) | A, B \in \mathbb{C}, A \neq B\}$.

Definition 2.1: A $[k \times \ell, \rho, \delta]$ *rank-metric code* is a linear code in $M_{k\times\ell}(\mathbb{F}_q)$ with dimension ρ and minimum rank distance δ.

The following theorem gives the Singleton bound for rank-metric codes.

Theorem 2.2: (T. Etzion and A. Vardy, [5]) For a $[k\times\ell, \rho, \delta]$ rank-metric code, we have $\rho \leq \min\{k(\ell-\delta+1), \ell(k-\delta+1)\}$.

A code that attains this bound is called a *maximum rank distance code* or an *MRD code*. The only previously known examples of MRD codes are the so-called Gabidulin codes.

Definition 2.3: Let $A \in M_{k\times\ell}(\mathbb{F}_q)$. The *lift* of A, denoted by $L(A)$, is the $k \times (k + \ell)$ standard matrix $(I_k\ A)$, where I_k is the $k \times k$ identity matrix.

The subspace generated by the rows of the lifted matrix $L(A)$ will be denoted by $\langle L(A)\rangle$. This subspace is in fact a rate-$k/(k + \ell)$ linear block code of length $k + \ell$ over $\mathbb{F}_q$.

There are at least two metrics that can be applied on the projective space $\mathcal{P}_q(n)$. The *subspace distance* is given by $d_S(A,B) = \dim A + \dim B - 2\dim(A \cap B)$. The next one is the *injection distance* which is given by $d_I(A,B) = \max\{\dim A, \dim B\} - \dim(A \cap B)$, for all $A, B \in \mathcal{P}_q(n)$. In this paper we shall use the subspace distance on the constructed Grassmannian codes.

A classic formula for the cardinality of the Grassmannian $\mathcal{G}_q(n,k)$ is given by the q-ary Gaussian coefficient

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}.$$

Definition 2.4: A Grassmannian code $\mathcal{C}$ in $\mathcal{G}_q(n,k)$ is called an $(n, M, d, k)_q$ code if $|\mathcal{C}| = M$ and its minimum subspace distance is d, where $d = \{\min d_S(U,V) | U, V \in \mathcal{C}, U \neq V\}$.

Definition 2.5: Let $\mathcal{C}$ be a $[k \times \ell]$ rank-metric code. The set

$$\begin{aligned} \Lambda(\mathcal{C}) &= \{\langle L(A) \rangle | A \in \mathcal{C}\} \\ &= \{\langle (I_k \ A) \rangle | A \in \mathcal{C}\} \end{aligned}$$

is called the *lift* of $\mathcal{C}$, which is clearly a Grassmannian code. The next theorem gives a more specific result.

Theorem 2.6: (A. Khaleghi and D. Silva and F. R. Kschischang, [8]) Let $\mathcal{C}$ be a $[k \times \ell, \rho, \delta]$ rank-metric code. The lift of $\mathcal{C}$ is a $(k+\ell, q^\rho, 2\delta, k)_q$ Grassmannian code.

The next results give bounds on the maximum number of codewords in a Grassmannian code.

Theorem 2.7: (T. Etzion and A. Vardy, [6]) Let $\mathcal{A}_q(n,d,k)$ be the maximum number of codewords of a code in $\mathcal{G}_q(n,k)$ with subspace distance $d = 2\delta + 2$. Then

$$\mathcal{A}_q(n, 2\delta+2, k) \leq \frac{\begin{bmatrix} n \\ k-\delta \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta \end{bmatrix}_q}.$$

Theorem 2.8: (A. Khaleghi, D. Silva, F. R. Kschischang, [8]) Let $\mathcal{A}_q(n,d,k)$ be the maximum number of codewords of a code in $\mathcal{G}_q(n,k)$ with injection distance d. Then

$$\mathcal{A}_q(n,d,k) \leq \frac{\begin{bmatrix} n \\ k-d+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-d+1 \end{bmatrix}_q}.$$

Theorems 2.7 and 2.8 are two existing versions of the *Anticode Bound* for Grassmannian codes.

If $A \in \mathbb{F}_q^n$, the *dual or orthogonal subspace* of A is given by $A^\perp = \{v \in V | u \cdot v = 0 \text{ for all } u \in A\}$ where $u \cdot v$ is the usual inner product between vectors u and v. As in the classical sense, there is the notion of duality in Grassmannian codes.

Definition 2.9: (R. Kötter and F. R. Kschichang, [9])

If $\mathcal{C} \subseteq \mathcal{G}_q(n,k)$ then its dual or complementary code is given by $\mathcal{C}^\perp = \{C^\perp \in \mathcal{G}_q(n, n-k) | C \in \mathcal{C}\}$.

Theorem 2.10: (R. Kötter and F. R. Kschichang, [9]) If $\mathcal{C}$ is an $(n, M, d, k)_q$ code then $\mathcal{C}^\perp$ is an $(n, M, d, n-k)_q$ code.

α	$w_{\mathtt{Ham}}(\alpha)$	$\phi(\alpha)$	$w_{\mathtt{B}}(\phi(\alpha))$	$w_R(\phi(\alpha))$
$(0,0)$	0	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	0	0
$(0,1)$	1	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	1	2
$(1,0)$	1	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	2
$(1,1)$	2	$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$	2	1
$(0,\omega)$	1	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	1	2
$(\omega,0)$	1	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	1	2
(ω,ω)	2	$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$	2	1
$(1,\omega)$	2	$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$	2	1
$(\omega,1)$	2	$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$	2	1
$(0,1+\omega)$	1	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	1	2
$(1+\omega,0)$	1	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	1	2
$(1,1+\omega)$	2	$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$	2	1
$(1+\omega,1)$	2	$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$	2	1
$(\omega,1+\omega)$	2	$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	2	1
$(1+\omega,\omega)$	2	$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	2	1
$(1+\omega,1+\omega)$	2	$\begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$	2	1

TABLE I
HAMMING WEIGHTS ON $\mathbb{F}_4^2$ AND BACHOC AND RANK WEIGHTS ON $M_2(\mathbb{F}_2)$

III. RANK-METRIC CODES AND GRASSMANNIAN CODES

Let $M_2(\mathbb{F}_p)$ be the non-commutative ring of 2×2 matrices over $\mathbb{F}_p$ and $GL(2,p)$ its multiplicative group of units. We now give the definition of the Bachoc weight $w_{\mathtt{B}}$ on $M_2(\mathbb{F}_p)$.
.

$$w_{\mathtt{B}}(A) = \begin{cases} 0 & \text{if } A = 0 \\ 1 & \text{if } A \in GL(2,p) \\ p & \text{otherwise} \end{cases}$$

In [2], an isometric map ϕ from $\mathbb{F}_4^2$ onto $M_2(\mathbb{F}_2)$ where

$$\phi((a+b\omega, c+d\omega)) = \begin{pmatrix} a+d & b+c \\ b+c+d & a+b+d \end{pmatrix}$$

was given using the Hamming weight $w_{\mathtt{Ham}}$ and the Bachoc weight $w_{\mathtt{B}}$ for $\mathbb{F}_4^2$ and $M_2(\mathbb{F}_2)$ respectively, such that $w_{\mathtt{Ham}}(\alpha) = w_{\mathtt{B}}(\phi(\alpha))$ for all $\alpha \in \mathbb{F}_4^2$.

Table I shows the elements of $\mathbb{F}_4^2$ with their corresponding Hamming weights and the elements of $M_2(\mathbb{F}_2)$ with their corresponding Bachoc and rank weights.

Lemma 3.1: Let $\mathcal{C}$ be a $[k \times \ell, \rho, \delta]$ rank-metric code with minimum nonzero rank Ω. Then $\delta = \Omega$.

Proof: Let $\mathcal{C}$ be a rank-metric code with minimum rank distance δ and minimum nonzero rank Ω. Let A and B be distinct elements of $\mathcal{C}$ such that rank$(A-B)$ is minimum. Note that rank$(A-B) \neq 0$. Then $\delta = d_R(A,B) = \text{rank}(A-B) \geq \Omega$. Moreover, let $A \in \mathcal{C}$ with minimum rank. Now, $\Omega = \text{rank}(A) = d_R(A,0) \geq \delta$. Thus, $\delta = \Omega$. □

Lemma 3.2: Let q be a power of a prime p. Then $\mathbb{F}_q^n$ is also an $\mathbb{F}_p$-vector space.

Lemma 3.3: Let $\phi : \left(\mathbb{F}_{p^2}\right)^2 \longrightarrow M_2(\mathbb{F}_p)$ where

$$\phi((a+b\omega, c+d\omega)) = \begin{pmatrix} a+d & b+c \\ b+c+d & a+b+d \end{pmatrix}.$$

Then ϕ is an isomorphism of $\mathbb{F}_p$-vector spaces.

Remark 3.4: From Lemma 3.3, if C is a linear block code of length 2 over $\mathbb{F}_{p^2}$ then $C \cong \phi(C)$ as $\mathbb{F}_p$-vector spaces.

For the following remark, let $\alpha_i = (a_i + b_i\omega, c_i + d_i\omega) \in \left(\mathbb{F}_{p^2}\right)^2$ and

$$A_i = \begin{pmatrix} a_i + d_i & b_i + c_i \\ b_i + c_i + d_i & a_i + b_i + d_i \end{pmatrix} \in M_2(\mathbb{F}_p)$$

where $1 \leq i \leq r$ for positive integer r.

Remark 3.5: Let r be a positive integer. Note that ϕ can be extended naturally in the following manner. We have $\phi : \left(\mathbb{F}_{p^2}\right)^{2r} \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi(\alpha_1, \alpha_2, ..., \alpha_{2r}) = \begin{pmatrix} A_1 & A_2 & ... & A_r \end{pmatrix}.$$

It is easy to see that $\left(\mathbb{F}_{p^2}\right)^{2r} \cong M_{2\times 2r}(\mathbb{F}_p)$ as $\mathbb{F}_p$-vector spaces. If C is a linear block code of length $2r$ over $\mathbb{F}_{p^2}$ then $C \cong \phi(C)$ as $\mathbb{F}_p$-vector spaces.

Lemma 3.6: (D. Falcunit, Jr. and V. Sison, [7]) If $p \equiv 2$ or 3 (mod 5) then the polynomial $f(x) = x^2 + x + (p-1)$ is irreducible over $\mathbb{F}_p$.

Theorem 3.7: Let C be a linear block code of length $2r$ over $\mathbb{F}_{p^2}$ and ρ its dimension as an $\mathbb{F}_{p^2}$-vector space. If $p \equiv 2$ or 3 (mod 5) and for all $(\alpha_1, \alpha_2, ..., \alpha_{2r}) \in C$, $\alpha_j = 0$ for each odd (resp. even) index j, then

i. $\phi(C)$ is a $[2 \times 2r, \rho, 2]$ rank-metric code,
ii. $\Lambda(\phi(C))$ is a $(2r+2, p^\rho, 4, 2)_p$ code, and;
iii. the pairwise intersection of codewords of $\Lambda(\phi(C))$ is trivial.

Proof: Let C be a linear block code of length n over $\mathbb{F}_{p^2}$. Note that by Remark 3.5, C and $\phi(C)$ are isomorphic as $\mathbb{F}_p$-vector spaces. Hence, the dimension of $\phi(C)$ is ρ. Moreover, let $(\alpha_1, \alpha_2, ..., \alpha_{2r}) \in C \backslash \{(0,0,...,0)\}$, $\alpha_j = 0$ for each odd (resp. even) integer j. To simplify the proof, we consider when $r = 1$ and hence we have $(0, \alpha_2) \in C \backslash \{(0,0)\}$. Note that $\alpha_2 = c + d\omega$ for some $c, d \in \mathbb{F}_p$. Then $\phi(0, c+d\omega) = \begin{pmatrix} d & c \\ c+d & d \end{pmatrix}$. Since c and d are not both zero, we have the following cases:

1. If $c = 0$ and $d \neq 0$ then the matrix becomes $\begin{pmatrix} d & 0 \\ d & d \end{pmatrix}$ with rank 2.
2. If $c \neq 0$ and $d = 0$ then the matrix becomes $\begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}$ with rank 2.
3. Let $c, d \neq 0$. Suppose rank of the matrix is not 2 then one row is a multiple of the other, that is, $(d,c) = x(c+d, d)$ for some $x \in \mathbb{F}_p$. This implies that $d = xc + xd$ and $c = xd$. Further, $d = x^2d + xd$ and $x^2 + x - 1 = 0$. Since $p \equiv 2$ or 3 (mod 5), by Lemma 3.6, $f(x) = x^2 + x - 1 = x^2 + x + (p-1)$ is irreducible over $\mathbb{F}_p$. Thus there is no $x \in \mathbb{F}_p$ such that $(d,c) = x(c+d, d)$ and hence the rank of the matrix is 2.

Thus, the minimum rank weight of $\phi(C)$ is 2. By Lemma 3.1, the minimum rank distance of $\phi(C)$ is also 2. It follows that $\phi(C)$ is a $[2 \times 2r, \rho, 2]$ rank-metric code.

It easy to see that (ii) follows directly from Theorem 2.6.

If $\Lambda(\phi(C))$ is a $(2r+2, p^\rho, 4, 2)_2$ code, the minimum subspace distance of $\Lambda(\phi(C))$ is 4. Let $A, B \in \Lambda(\phi(C))$. Note that $\dim A = \dim B = 2$ and we have $4 \leq d_S(A,B) = \dim A + \dim B - 2\dim(A \cap B)$. Thus, $4 \leq 2 + 2 - 2\dim(A \cap B)$ and hence $\dim(A \cap B) \leq 0$. Therefore, $\dim(A \cap B) = 0$. This means that the pairwise intersection of codewords of $\Lambda(\phi(C))$ is trivial. □

Remark 3.8: Let r be a positive integer and consider

$$S = \{(0, c_1 + d_1\omega, 0, c_2 + d_2\omega, 0, ..., 0, c_r + d_r\omega) | c_i, d_i \in \mathbb{F}_p\},$$

a subspace of $\left(\mathbb{F}_{p^2}\right)^{2r}$ as an $\mathbb{F}_p$-vector space. By Theorem 3.7, we can consider the map $\phi : S \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi((0, c_1 + d_1\omega, 0, c_2 + d_2\omega, ..., 0, c_r + d_r\omega)) = \begin{pmatrix} d_1 & c_1 & d_2 & c_2 & ... & d_r & c_r \\ c_1 + d_1 & d_1 & c_2 + d_2 & d_2 & ... & c_r + d_r & d_r \end{pmatrix}$$

as the map $\phi_O : \left(\mathbb{F}_{p^2}\right)^r \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi_O((c_1 + d_1\omega, c_2 + d_2\omega, ..., c_r + d_r\omega)) = \begin{pmatrix} d_1 & c_1 & d_2 & c_2 & ... & d_r & c_r \\ c_1 + d_1 & d_1 & c_2 + d_2 & d_2 & ... & c_r + d_r & d_r \end{pmatrix}.$$

Note that $\phi(S) = \phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ and hence the rank of each nonzero element of $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ is 2. Since the odd positions of S are all zeros, we can collapse the elements in such a way that the entries in the odd positions are deleted and hence we can look at the elements of S as simply elements of $\left(\mathbb{F}_{p^2}\right)^r$.

In an analogous manner consider

$$\overline{S} = \{(a_1 + b_1\omega, 0, a_2 + b_2\omega, 0, ..., a_r + b_r\omega, 0) | a_i, b_i \in \mathbb{F}_p\},$$

which is also a subspace of $\left(\mathbb{F}_{p^2}\right)^{2r}$ as an $\mathbb{F}_p$-vector space. By Theorem 3.7 iv, we can look at $\phi : \overline{S} \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi((a_1 + b_1\omega, 0, a_2 + b_2\omega, 0, ..., a_r + b_r\omega, 0)) = \begin{pmatrix} a_1 & b_1 & a_2 & b_2 & ... & a_r & b_r \\ b_1 & a_1 + b_1 & b_2 & a_2 + b_2 & ... & b_r & a_r + b_r \end{pmatrix}$$

as $\phi_E : \left(\mathbb{F}_{p^2}\right)^r \longrightarrow M_{2\times 2r}(\mathbb{F}_p)$ where

$$\phi_E((a_1 + b_1\omega, a_2 + b_2\omega, ..., a_r + b_r\omega)) = \begin{pmatrix} a_1 & b_1 & a_2 & b_2 & ... & a_r & b_r \\ b_1 & a_1 + b_1 & b_2 & a_2 + b_2 & ... & b_r & a_r + b_r \end{pmatrix}.$$

Similarly, $\phi(\overline{S}) = \phi_E(\left(\mathbb{F}_{p^2}\right)^r)$ and the rank of each nonzero element of $\phi_E(\left(\mathbb{F}_{p^2}\right)^r)$ is 2. Since the even positions of S are all zeros, we can collapse the elements in such a way that the entries in the even positions are deleted and hence we can look at the elements of $\overline{S}$ as simply elements of $\left(\mathbb{F}_{p^2}\right)^r$ as well.

Theorem 3.9: For prime p where $p \equiv 2$ or 3 (mod 5) and for any positive integer r, the rank-metric code $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ satisfies the Singleton bound.

Proof: Let p be prime such that $p \equiv 2$ or 3 (mod 5), r be a positive integer, and ρ be the dimension of $\left(\mathbb{F}_{p^2}\right)^r$ as an $\mathbb{F}_p$-vector space. From Remark 3.8 and Theorem 3.7, $\phi_O(\left(\mathbb{F}_{p^2}\right)^r)$ is a $[2 \times 2r, \rho, 2]$ rank-metric code. Note that $\left|\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)\right| = p^\rho$ and $\left|\left(\mathbb{F}_{p^2}\right)^r\right| = p^{2r}$ but $\left|\left(\mathbb{F}_{p^2}\right)^r\right| = \left|\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)\right|$. Hence it follows that $\rho = 2r$. Now, a $[k \times \ell, \rho, \delta]$ rank-metric code satisfies the Singleton bound if

$$\rho \leq \min\{k(\ell - \delta + 1), \ell(k - \delta + 1)\}.$$

Substituting the values,

$$\begin{aligned} 2r &\leq \min\{2(2r - 2 + 1), 2r(2 - 2 + 1)\} \\ 2r &\leq \min\{4r - 2, 2r\}. \end{aligned}$$

Note that $4r - 2 \geq 2r$ for $r \geq 1$. Thus, for prime p where $p \equiv 2$ or 3 (mod 5) and for any positive integer r, $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ satisfies the Singleton bound for rank-metric codes and hence a maximum rank distance code. □

A MAGMA program was designed to obtain the maximum rank distance code $\phi_O\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ for $p = 2$ and for any positive integer r.

In a similar manner we can prove that $\phi_E\left(\left(\mathbb{F}_{p^2}\right)^r\right)$ also satisfies the Singleton bound for any positive integer r.

Example 3.10: Consider $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$. We have

$$\phi_O(\mathbb{F}_4) = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right\}.$$

Note that by Theorem 3.7 and Remark 3.8, $\phi_O(\mathbb{F}_4)$ is a $[2 \times 2, 2, 2]$ rank-metric code. By Theorem 3.9, $\phi_O(\mathbb{F}_4)$ is a maximum rank distance code.

Example 3.11: Again, consider $\mathbb{F}_4 = \{0, 1, \omega, 1 + \omega\}$. We have

$$\phi_E(\mathbb{F}_4) = \left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\right\}.$$

Note that by Theorem 3.7 and Remark 3.8, $\phi_E(\mathbb{F}_4)$ is a $[2 \times 2, 2, 2]$ rank-metric code, and a maximum rank distance code.

Now, let $T = \{(0, c + d\omega) | c, d \in \mathbb{F}_3\}$. Table II shows the elements of T and their corresponding images in $M_2(\mathbb{F}_3)$ under ϕ with their rank weights. From the given table, each nonzero element of $\phi(T)$ has rank 2.

Example 3.12: Refer to Table II, $\phi(T) = \phi_O(\mathbb{F}_9)$ is a $[2 \times 2, 2, 2]$ rank-metric code. By Theorem 3.9, $\phi_O(\mathbb{F}_9)$ is a maximum rank distance code.

Note that the first prime that does not satisfy Theorem 3.9 is $p = 5$. We have $5 \equiv 0$ (mod 5). Now, $2 + \omega \in \mathbb{F}_{5^2} = \mathbb{F}_{25}$ and $\phi_O(1 + 2\omega) = \begin{pmatrix} 1 & 2 \\ 3 & 1 \end{pmatrix}$ whose rank is 1. Therefore, $\phi_O(\mathbb{F}_{25})$ cannot be a rank-metric code with minimum distance 2.

Definition 3.13: Let r and m be positive integers. the matrix $H_m = \begin{pmatrix} I_m & 0_{m \times mr} \end{pmatrix}$ and the matrix $\widehat{H}_m = \begin{pmatrix} 0_{m \times mr} & I_m \end{pmatrix}$, where I_m is the $m \times m$ identity matrix and $0_{m \times mr}$ is the $m \times mr$ zero matrix.

α	$\phi(\alpha)$	$w_R(\phi(\alpha))$
$(0,0)$	$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$	0
$(0,1)$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2
$(0,\omega)$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	2
$(0,1+\omega)$	$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$	2
$(0,2)$	$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$	2
$(0,2\omega)$	$\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}$	2
$(0,1+2\omega)$	$\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$	2
$(0,2+2\omega)$	$\begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$	2
$(0,2+\omega)$	$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$	2

TABLE II
ELEMENTS OF $T = \{(0, c + d\omega) | c, d \in \mathbb{F}_3\}$ AND THEIR IMAGES UNDER ϕ WITH THEIR RANK WEIGHTS

Remark 3.14 (Anticode Bound):

$$\mathcal{A}_p(2r + 2, 4, 2) \leq \frac{p^{2r+2} - 1}{p^2 - 1}$$

Remark 3.15: For any natural number r, we have

$$1 + p^2 + p^4 + p^6 + ... + p^{2r} = \frac{p^{2r+2} - 1}{p^2 - 1}.$$

Theorem 3.16: Let p be prime where $p \equiv 2$ or 3 (mod 5), r be a positive integer, and consider a class of $\mathbb{F}_p$-vector spaces $\left\{\left(\mathbb{F}_{p^2}\right)^i | i = 1, 2, ..., r\right\}$. Let D_i be the set of vectors that contain $\Lambda\left(\phi_O\left(\mathbb{F}_{p^2}\right)^i\right)$ such that the vectors are appended with zeros in the left so that they have common length $2r + 2$. Then $G_p(r, 2) = \left\langle \widehat{H}_2 \right\rangle \bigcup \left(\bigcup_{i=1}^{r} D_i\right)$ is a $\left(2r + 2, \frac{p^{2r+2} - 1}{p^2 - 1}, 4, 2\right)_p$ code.

Proof: For $1 \leq i \leq r$, let D_i be the set of vectors that contain $\Lambda(\phi_O(\mathbb{F}_4^i))$ such that the vectors are appended with zeros in the left so that they have common length $2r + 2$. Note that $\left|\Lambda\left(\phi_O\left(\left(\mathbb{F}_{p^2}\right)^i\right)\right)\right| = \left|\phi_O\left(\left(\mathbb{F}_{p^2}\right)^i\right)\right| = \left|\left(\mathbb{F}_{p^2}\right)^i\right| = p^{2i}$. Now,

$$\left|\bigcup_{i=1}^{r} D_i\right| = p^2 + p^4 + p^6 + ... + p^{2r}.$$

Let $G_p(r, 2) = \left\langle \widehat{H}_2 \right\rangle \bigcup \left(\bigcup_{i=1}^{r} D_i\right)$ so that by Remark 3.15,

$$|C| = 1 + p^2 + p^4 + p^6 + ... + p^{2r} = \frac{p^{2r+2} - 1}{p^2 - 1}.$$

Note that the only intersection of the D_i's is just the zero space. Moreover, the only intersection of $\left\langle \widehat{H}_2 \right\rangle$ with the D_i's is also trivial. Thus, the obtained code is a $\left(2r+2, \frac{p^{2r+2}-1}{p^2-1}, 4, 2\right)_p$ code. □

Remark 3.17: The code $G_p(r,2)$ obtained in Theorem 3.16 attains the Anticode bound given in Remark 3.14.

Similarly we can also obtain a $\left(2r+2, \frac{p^{2r+2}-1}{p^2-1}, 4, 2\right)_p$ code using the mapping ϕ_E.

Example 3.18: Let $p = 2$ and $r = 1$. We have $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}$. Now the lifted matrices of $\phi_O(\mathbb{F}_4)$ are $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$. Then the elements of $G_2(1,2)$ are

$$C_1 = \{(1,0,0,0), (0,1,0,0), (1,1,0,0), (0,0,0,0)\},$$
$$C_2 = \{(1,0,0,1), (0,1,1,0), (1,1,1,1), (0,0,0,0)\},$$
$$C_3 = \{(1,0,1,0), (0,1,1,1), (1,1,0,1), (0,0,0,0)\},$$
$$C_4 = \{(1,0,1,1), (0,1,0,1), (1,1,1,0), (0,0,0,0)\}, \text{ and;}$$
$$C_5 = \{(0,0,1,0), (0,0,0,1), (0,0,1,1), (0,0,0,0)\}.$$

Note that $G_2(1,2)$ is a $(4,5,4,2)_2$ code. Now, when $p = 2$ and $r = 1$, the Anticode bound becomes $\frac{2^{2+2}-1}{3} = 5$. Thus, $G_2(1,2)$ attains this bound.

Example 3.19: Again, consider $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\}$. Now the lifted matrices of $\phi_E(\mathbb{F}_4)$ are $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$. Then the elements of the Grassmannian code $\mathcal{C}$ generated by the lifted matrices, with $C_5 = \left\langle \widehat{H}_2 \right\rangle$ are given by

$$C_1 = \{(1,0,0,0), (0,1,0,0), (1,1,0,0), (0,0,0,0)\},$$
$$C_2 = \{(1,0,1,0), (0,1,0,1), (1,1,1,1), (0,0,0,0)\},$$
$$C_3 = \{(1,0,0,1), (0,1,1,1), (1,1,1,0), (0,0,0,0)\},$$
$$C_4 = \{(1,0,1,1), (0,1,1,0), (1,1,0,1), (0,0,0,0)\}, \text{ and;}$$
$$C_5 = \{(0,0,1,0), (0,0,0,1), (0,0,1,1), (0,0,0,0)\}.$$

Note that $\mathcal{C}$ is also a $(4,5,4,2)_2$ code that attains the Anticode bound.

Corollary 3.20: The dual of $G_p(r,2)$ is a $\left(2r+2, \frac{p^{2r+2}-1}{p^2-1}, 4, 2r\right)_p$ code.

Proof: This directly follows from Theorem 2.10. □

MAGMA programs were created to obtain the anticode-optimal code $G_p(r,2)$ and its dual in Theorem 3.16 and Corollary 3.20 for $p = 2$ and for any positive integer r.

IV. Graphs of Anticode-Optimal Grassmannian Codes $G_p(r,2)$

A *graph* G is a pair (V,E) where V is a finite set whose members are called *vertices*, and E is a subset of the set $V \times V$ of unordered pairs of vertices. The members of E are called *edges* [3]. If $\{v, w\}$ is an edge of G, the vertices v and w are said to be *adjacent*. An edge with identical ends is called a *loop* and an edge with distinct ends is called a *link*. A graph is *simple* if it has no loops and no two of its links join the same pair of vertices. In a simple graph, the *degree* of a vertex $v \in G$ is the number of edges of G incident with v [4].

A simple graph in which each pair of distinct vertices is joined by an edge is called a *complete graph*. A complete graph with N vertices is denoted by K_N. The complete graph of N vertices has $\frac{N(N-1)}{2}$ edges. The degree of any vertex in K_N is $N-1$.

Note that for distinct $A, B \in G_p(r,2)$ in Theorem 3.16, we have $A \cap B = \{0\}$.

Definition 4.1: Let the subspaces of $G_p(r,2)$ be the vertices of the graph $\Gamma_p(r,2)$. Two vertices A and B are adjacent if and only if $\dim(A \cap B) = 0$.

It follows that the edge set of $\Gamma_p(r,2)$ is the set of all unordered distinct pair of vertices.

Theorem 4.2: The graph $\Gamma_p(r,2)$ is a complete graph with $\frac{p^{2r+2}-1}{p^2-1}$ vertices.

Proof: Note that $|G_p(r,2)| = \frac{p^{2r+2}-1}{p^2-1}$ so $\Gamma_p(r,2)$ has $\frac{p^{2r+2}-1}{p^2-1}$ vertices. Since the intersection of any two subspaces in $G_p(r,2)$ is trivial, its dimension is zero. Thus, each pair of vertices is joined by an edge. By definition, $\Gamma_p(r,2)$ is a complete graph with $\frac{p^{2r+2}-1}{p^2-1}$ vertices. □

Remark 4.3: We can easily compute the number of edges of $\Gamma_p(r,2)$ and the degree of each vertex.

Example 4.4: When $p = 2$ and $r = 2$, we have a $(4,21,4,2)_2$ code. The associated graph $\Gamma_2(2,2)$ of the $(4,21,4,2)_2$ code is a complete graph with 21 vertices. The number of edges is 210 and the degree of each vertex is 20.

References

[1] R. Ahlswede and N. Cai and S.-Y. Li and R. Yeung, "Network information flow", *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204-1216, 2000.

[2] C. Bachoc, "Application of coding theory to the construction of modular lattices," *J. Combinatorial Theory*, vol. 78, pp. 92-119, 1997.

[3] N. L. Biggs and A. T. White, Permutation Groups and Combinatorial Structures, Cambridge University Press, New York, 1979.

[4] J. A. Bondy and U. S. R. Murty, Graph Theory With Applications, *Elsevier Science Publishing Co., Inc.*, New York, 1976.

[5] T. Etzion, "Subspace codes – bounds and constructions", *1st European Training School on Network Coding, Bacelona, Spain*, February 2013.

[6] T. Etzion and A. Vardy, Error-correcting codes in projective space, *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 1165-1173, February 2011.

[7] D. Falcunit, Jr. and V. Sison, Cyclic Codes over the Matrix Ring $M_2(\mathbb{F}_p)$ and their Isometric Images over $\mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$, *Proceedings of the 2014 International Zürich Seminar on Communications, Sorell Hotel Zürichberg, Zürich, Switzerland*, pp. 91-96, 26-28 February 2014.

[8] A. Khaleghi and D. Silva and F. R. Kschischang, Subspace Codes, *IMA Int. Conf.*, vol. 49, no. 4, pp. 1-21, 2009.

[9] R. Kötter and F. R. Kschichang, Coding for errors and erasures in random network coding, *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3579-3591, 2008.